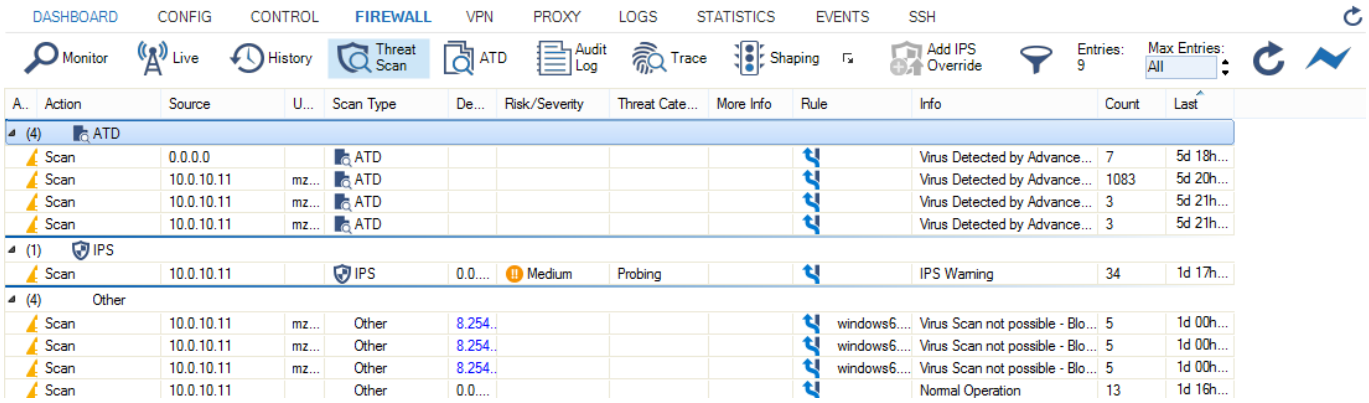
How to Manage Threats

https://campus.barracuda.com/doc/43847234/

Threats that are detected by the IPS engine are listed in the **Threat Scan** tab of the **FIREWALL** page of a Barracuda NG Firewall. This user interface provides a detailed view of information to each detected threat.

Firewall Threat Scan Interface



The **Threat Scan** interface can also be used to detect and manage false positive detections. If one of the entries listed was detected as malicious but should be allowed instead,

1. Select the desired entry.
2. Select **Add IPS Overrides** in the upper bar.
3. In the **False Positive** interface, click **Send Changes** and **Activate**.

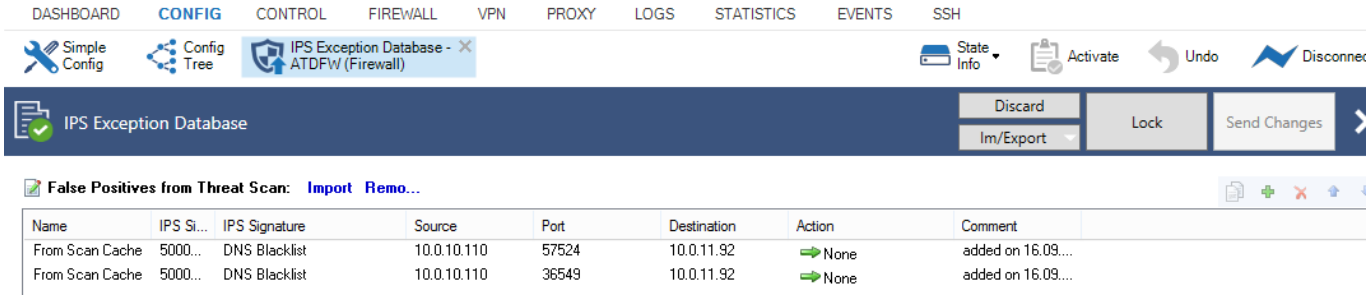
The entries are added to the IPS False Positives list of the Barracuda NG Firewall and, if present, to the Barracuda NG Control Center where you can import them. Entries added to the IPS False Positives list will automatically get the **None** action and can be edited in the **IPS False Positive** interface.

IPS Exceptions

With IPS enabled, it may happen that the engine detects network traffic that seems to be suspicious, but in special circumstances needs to be allowed by the system administrator. To manage these threats, proceed as follows:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > IPS Exception Database**.

2. Click **Lock**.



By selecting an entry, further modifications can be done by simply clicking the desired cell in the table. To extend a matching policy it is possible to enter * (ALL) in the columns **IPS Signature ID**, **Source**, **Port** and **Destination**. A blank cell represents * (All). It is also possible to manually create or copy false positives entries. To do so, click **Add** to create a new entry and configure as desired.

Figures

1. threat_scan.png
2. f_pos.png